

REMARKS

Claims 1-6 are pending in the application. Claims 1-3 stand rejected under §103 as unpatentable over U.S. Patent No. 6,959,390 to Challener in view of U.S. Patent No. 6,947,556 to Matyas. Claims 4-6 stand rejected as unpatentable over Challener in view of Matyas and further in view of U.S. Patent Pub. No. 2002/0007454 of Tarpenning. For the reasons set forth below, reconsideration of the application is respectfully requested.

One principal difference between applicant's claimed invention and the technology disclosed by the cited prior art is that applicant's claimed invention relates to methods of communicating between two computer systems wherein both a public key and a private key are sent from a first system (call it the certification generating system) to a second system (call it the user system), while the cited prior art relates to methods of communicating between two computer systems wherein only a public key is sent from the certification generating system to the user system. This difference is clearly set forth in the background to the present invention, which notes that the claimed invention addresses drawbacks presented by the prior art "one direction" systems.

Accordingly, it is believed that the present invention is patentable over the cited prior art because the claimed invention includes the limitation "sending the public key and the encrypted private key to a user unit". That limitation is neither taught nor suggested by the cited prior art.

More particularly describing the prior art systems that are the subject of the reference, in the system the certificate generating system sends a public key to a user's system. The user's system then uses that public key to encrypt a message to be sent to

the certificate generating system. The encrypted message is received by the certificate generating system, which then uses a corresponding private key to decrypt the message. The important thing to recognize is that the private key is never sent to the user's system. This fact is explicitly stated in the Challenger reference, for example at col. 5, lines 36 through 38, where it states: "[t]he encryption engine does not make the decrypted private key available to any service, application, or device."

Of course, the Challenger patent is not directed to the described system per se, but is instead directed to a method of storing the private key in a non-secure storage device of the certification generating system. Nevertheless, the fact remains that in the system disclosed by Challenger, the private key is never sent to the user's system – it is instead stored only in the certificate generating system.

Applicant's claimed invention addresses a drawback of the system described by Challenger, namely, that messages between the certification generating system and the user's system are secure in only one direction. To address this drawback the present invention proposes a system in which both a public key and a private key are sent from the certification generation system to the user's system. In this system, the private key is first encrypted and is then sent along with the public key from the certification generation system to the user's system.

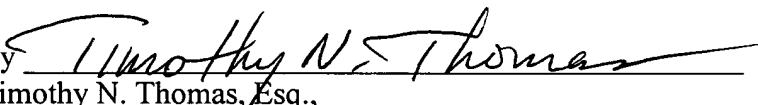
In view of the above it can be seen that the claimed invention includes at least one limitation that is neither taught nor suggested by the cited prior art. That limitation has been rewritten in the pending claims to further highlight the difference described above. Accordingly, the claimed invention now states that the claimed invention requires "sending the public key and the encrypted private key to a user unit." Again, that

limitation is not taught nor suggested by the prior art. The prior art simply does not send the private key to the user unit, and has no reason to do so.

Looking beyond the Challenger reference, none of the other cited prior art appears to disclose a system where both public and private keys are sent from a certificate generation system to a user system to provide two-way secure communication. Therefore, combining either Matyas or Tarpenning with Challenger would not appear to teach or suggest applicant's claimed invention.

In view of the foregoing, it is respectfully submitted that the rejections under §103 should be withdrawn and the application should be passed to allowance. Such action is respectfully solicited.

Respectfully submitted,

By 
Timothy N. Thomas, Esq.,
Reg. No. 35,714
Woodard, Emhardt, Moriarty, McNett & Henry LLP
111 Monument Circle, Suite 3700
Indianapolis, IN 46204-5137
(317) 634-3456 Telephone
(317) 637-7561 Facsimile

Attorney for Applicant